UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003

21254 7590 06/22/2007

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
06/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/457,732	CALIFANO ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-9 and 11-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-9 and 11-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment received on 16 January 2007 constitutes a withdrawal of the appeal and reopens prosecution as described at the conclusion of the Examiner's Answer of 13 November 2006.

2. Claims 1, 5-9, and 11-36 have been presented for examination.

3. Claims 2-4 and 10 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments filed 16 January 2007 have been fully considered but they are not persuasive.

5. In response to the Applicant's position that the Examiner did not respond to or answer the substance of the Applicant's traversal, the Examiner disagrees. In response to a proper 35 U.S.C. 101 rejection, the burden shifts to the applicant to rebut the prima facie showing. The Applicant may rebut this rejection using any combination of the following: amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication. In response to the requirement, the Applicant did not amend the claims, submit an affidavit or declaration, or a printed publication to rebut the Examiner's rejection. Instead the Applicant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close. The Applicant is reminded that the features upon which applicant relies, such as the methods disclosed in the specification, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner has considered the

specification, claims, and prior art before making the rejection and believes the asserted utility would be incredible to a person of ordinary skill in the art. See *In re Rinehart*, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

6. The Applicant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention and the Examiner responded in the only method available at the time, and as such the rejection should be maintained.

7. In response to the Applicant's arguments that the Examiner is not considering the Applicant's actual argument or the actual disclosure of the invention, the Examiner disagrees. The Applicant agrees with the Examiner's position that a simple hash function would not work on page 26 of the Appeal Brief filed 07 September 2006. The Applicant refers to methods for circumventing the problems of comparing encrypted or hashed data samples but is reminded that the features upon which applicant relies are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner would like to point out that the Applicant fails to define/redefine the term hash function to coincide with a particular method disclosed in the specification. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Applicant has not elaborated in the claim language that the hash function is one of the disclosed methods on pages 17-20 of the

specification. The Applicant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must " set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the art notice of the change" in meaning.

8. The Examiner has considered the claim language as a whole and in light of the specification, and has refrained from reading limitations from the specification into the claim language, especially giving the "hash function" its broadest reasonable interpretation. The Examiner does not disagree with the Applicant that the disclosure of the invention is operable, but the claim language as broadly interpreted by the Examiner provides for an inoperable invention and the rejection should be maintained.

9. In response to applicant's argument that the claimed invention provides a method and system for processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

10. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features, such as how the comparison between the two data sets are compared, upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification

are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Applicant does not claim the structure that does the comparing between the two encrypted samples, but instead claims the method steps which the Examiner has shown to be taught by *Borza*.

11. In response to the Applicant's arguments that *Borza* does not determine whether h(P) is close to h(P`), the Examiner disagrees. *Borza* discloses at column 16, lines 19-38 discloses techniques for determining the identification of someone by acquiring a biometric sample and comparing it to the stored templates. If the sample acquired for authentication is within predetermined range of the template, identification is provided for, if it is outside that predetermined range, then the user is not authenticated. *Borza* teaches comparing encrypted samples to encrypted templates in column 8, lines 28-38. The Applicant is reminded of MPEP 2123, which states that patents are relevant as prior art for all they contain.

12. *Borza* discloses determining whether h(P) is close to h(P`), without having to be identical matches, when comparing encrypted samples to encrypted templates, and the rejection should be maintained.

13. In response to the Applicant's argument that *Kharon* does not disclose extracting multiple subsets of data. In column 14, lines 40-53 *Kharon* discloses the k^{th} minutia and groupings of minutia. *Kharon* also states at column 13, lines 63-67 that the data set is defined so that N represents the total number of minutia for the fingerprint.

14. *Kharon* discloses extracting multiple subsets from the data in disclosing multiple instances of the minutia, and the rejection should be upheld.

15. In response to the Applicant's argument that *Kharon* does not teaches comparing encrypted versions of the sub-collection with those stored in the database, the Examiner disagrees. As shown above, *Borza* provides a showing of comparing two encrypted data sets for authentication purposes. *Kharon* teaches at column 14, lines 1-9 of comparing the minutia data sets to that of a database for authenticating the fingerprint.

16. Therefore, the combination of references discloses comparing encrypted subsets of data against a database for verification and the rejection should be maintained.

17. In response to applicant's argument that the claimed invention using a smaller subset of data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data sets, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

18. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

19. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*,.800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

20. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as extracting

subsets of data and comparing encrypted subsets of data, are not recited in all of the rejected independent claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

21. In response to the Applicant's arguments that the amendment's to the claims overcomes the 35 U.S.C. 101 rejection of claims 31-36, the Examiner disagrees. The Examiner interprets the term "computer-readable medium" to draw support from page 23 of the specification which discloses a machine-readable data storage medium which includes, but is not limited to a DASD storage, magnetic tape, electronic read-only memory, an optical storage device, paper "punch" cards, or other suitable signal bearing media including transmission media such as digital and analog and communication links and wireless. The Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection and the rejection is maintained. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

22. See further rejections that follow.

Specification

23. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: There is a lack of antecedent basis for the term "computer-readable medium" in claims 31-36, the closest support that can be found is on page 23 of the specification which discloses a machine-readable data storage medium which includes, but is not limited to a

DASD storage, magnetic tape, electronic read-only memory, an optical storage device, paper "punch" cards, or other suitable signal bearing media including transmission media such as digital and analog and communication links and wireless.

Claim Rejections - 35 USC § 101

24. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

25. Claims 1, 14-16, 31, and 32 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claims 1, 14-16, 31, and 32 all generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication. The Examiner holds that such a method could not work, as evident by the **Handbook of Applied Cryptography** to Menezes et al., hereinafter Menezes. Chapter 9 of Menezes discloses the properties of hash functions. On page 331, Menezes proceeds to state one of the properties of one-way hash functions being near-collision resistance. Near-collision resistance is the property that states that "it should be hard to find any two inputs x, x' such that $h(x)$ and $h(x')$ differ in only a small number of bits." This is further supported by section **9.2.2 Basic properties and definitions**, on page 323 and 324.

26. Claims 31-36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. On page 23 of the Specification, the Applicant describes a computer-readable medium (as discussed above drawn to the machine readable data storage medium) as being a transmission medium, such as digital and analog and communication links and wireless. The Office's current position is that claims involving signals encoded with

functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claim Rejections - 35 USC § 103

27. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

28. Claims 1, 5-9, 11-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,446,210 to Borza, hereinafter Borza, in view of U.S. Patent No. 6,487,662 to Kharon et al., hereinafter Kharon.

29. As per claims 1, 13, 14, 16, 18, 20, 24-26, 28, 30-32, 34, and 36, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53);

obtaining a sample of P' such that a comparison can be made (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

at least one of obtaining and computing h(P') (Figure 5; column 7, line 45 to column 8, line 3); and

to determine whether P' is close to a predetermined subject, comparing h(P) to all available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P (Figures 12, 13, 16, 17; column 8, lines 28-38, column 14, lines 21-59, column 16, lines 31-37, column 16, lines 53-58, i.e. "when the value is within predetermined limits for an acceptable value, identification is provided....when the value falls outside the predetermined limits identification is not provided");

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

wherein said semiotic data comprises biometric data (column 11, line 65 to column 12, line 18);

wherein said function h comprises a secure hash function (Figure 5; column 7, line 45 to column 8, line 3);

wherein the data set P is not determined perfectly by its reading (column 8, lines 28-38, column 14, lines 21-59, column 16, lines 61-37, column 16, lines 53-58)

wherein each reading gives a number Pi, wherein I is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 8, lines 28-48; column 11, lines 25-34; column 12, lines 25-61),

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possibly by a direct comparison of the encrypted data (Figures 7b, 9-11, 14, 18; column 13, lines 1-21, column 14, line 60 to column 15, line 63, column 16, line 58 to column 17, line 14),

each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61),

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user (column 4, lines 46-58; column 5, lines 42-55),

wherein at least one of said data set P and P` comprises a personal data set (column 12, lines 25-34).

30. Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

31. Kharon teaches further comprising:

extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67);

comparing encrypted versions of the sub-collections Sj with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

32. As per claim 5, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

the method further comprising:

selecting a private key/public key (K, k) once for all cases (column 4, lines 26-32); and

choosing said function h as the public encryption function corresponding to k (column 5, lines 28-54).

33. Borza does not teach destroying said private key K and sending said private key K to a trusted party. It would have been obvious to one having ordinary skill in the art at the time the invention was made to destroy the private key K and send it the private key K to a trusted third

party, since it is known in the art that the private key is needed to decrypt any message encrypted with public key k, therefore the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k.

34. Regarding claim 6, Borza teaches wherein said data set P cannot be extracted from h(P), except by the trusted party (column 8, lines 28-38).

35. Regarding claim 7, Borza teaches to determine whether some P' is a predetermined subject, comparing said h(P) to all available h(P)s (column 12, lines 48-61); and

determining whether there is a match (column 12, lines 48-61).

36. Regarding claim 8, Borza does not teach wherein the trusted party comprises a panel of members, and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the trusted party to comprise of a panel of members, and share a secret is amongst the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret, since it has been held that mere duplication of essential elements (e.g. trusted third party) involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.,* 193 USPQ 8. See also MPEP § 2144.04.

37. As per claim 9, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

wherein the data set P is not determined perfectly by its reading (column 11, lines 25-34),

wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

38. Borza does not disclose extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

39. Kharon teaches extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller

section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

40. With regards to claims 11 and 21, Borza does not teach comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

41. Kharon teaches comparing encrypted versions of the sub-collections Sj with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

42. Concerning claims 12 and 23, Borza teaches each time a Pi, with $i > 0$, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61).

43. As per claims 15, 17, 27, and 33, Borza teaches a method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29);

storing each of the at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38),

to determine whether a data set P` is a predetermined subject, comparing an encrypted data set of P` to the at least one encrypted data set stored in the database to determine whether there is a match (Figure 12; column 8, lines 28-38).

44. Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability; comparing encrypted versions of the sub-collections Sj with those data stored in said database.

45. Kharon teaches extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67);

comparing encrypted versions of the sub-collections Sj with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

46. As per claims 19, 29, and 35, Borza teaches a method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29); and

storing each said at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38).

47. Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

48. Kharon teaches further comprising:

extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

49. Regarding claim 22, Borza teaches wherein the data set P is not determined perfectly by its reading, such that each reading gives a number Pi,

wherein i is no less than 0 (column 11, line 65 to column 12, line 34),

wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

Conclusion

50. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

51. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

52. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

53. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

54. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100